Claims

1. A method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve conditional access to at least one of valuable contents and services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip, characterized in that said external memory and said chip are uniquely linked by encrypting sensitive application code and data with a secret key stored in a secured memory area of the internal memory, the encrypted code and data being then stored in said external memory.

2. The method of claim 1, wherein a random number and a hash value of the random number are also encrypted with said secret key and stored in the external memory, the encrypted random number and hash value are decrypted with the secret key at least on each reset of the device, and decryption of the encrypted sensitive code and data are only allowed if the decrypted hash value equals a hash value calculated from the decrypted random number.

3. The method of claim 1 or claim 2, characterized in that application code down-loaded into the device is signed with a private key of an asymmetric key pair and proper execution of the application is subject to a verification of the signature with a public key of said key pair.

4. The method of claim 3, wherein the signature is generated by obtaining a hash value from said application code and encrypting the hash value with the private key.

5. The method of claim 3 or claim 4, wherein the public key of said key pair is stored in an internal read only memory of the device.

6. The method of claim 3 or claim 4, wherein the public key of said key pair is stored in an internal secured memory area of the device.

7. The method of claim 3 or claim 4, wherein a secure architecture designer's public key is stored in an internal read only memory of the device, a customer's public key is signed with the designer's private key and stored in the external memory, the customer's public key is retrieved by decrypting with the designer's public key read from the read only memory, the encrypted customer's public key read from the external memory, and the signature is verified.

8. The method of claim 3 or claim 4, wherein the public key of said key pair is downloaded with the signed application code and a hash value of the public key is encrypted with a private key the corresponding public key of which is stored in internal read only memory of the device, and the encrypted hash value is also downloaded to the device.

9. The method of any of claims 1 to 8, wherein the application code is downloaded into the device, encrypted with the secret key and stored in the external memory.

10. A method of protecting a device against unintended use in a secure environment, the device being adapted to execute applications that involve secure transactions and/or conditional access to valuable contents and/or services, and the device including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip;

characterized in that

a) any application code down-loaded into the device is signed with a private key of an asymmetric key pair and proper execution of the application is subject to a verification of the signature with a public key of said key pair;

b) said external memory and said chip are uniquely linked by encrypting sensitive application code and data with a secret key stored in a secured memory area of the internal memory and storing the encrypted code and data in the external memory;

c) a random number and a hash value of the random number are also encrypted with said secret key and stored in the external memory;

d) on each reset of the device, the encrypted random number and hash value are decrypted with the secret key, and decryption of the encrypted sensitive code and data are only allowed if the decrypted hash value equals a hash value calculated from the decrypted random number.

11. A method according to any of the preceding claims, characterized in that, after manufacturing of the chip and prior to delivery to a customer, a secret access channel is established to write a secret personalization key into the secure memory area.

12. The method of claim 11, wherein the content of the secure memory area is protected by calculating a hash value of the secure memory area content and writing the hash value into the secure memory area.

13. The method of claim 11 or 12, wherein a personalization application is signed with a Secure Architecture Designer's private key and then encrypted with the secret personalization key, the personalization application is loaded into the device and decrypted with the secret personalization key, the signature of the personalization application is checked with the Secure Architecture Designer's public key, and the personalization application is executed to write sensitive personalization data into the secure memory area.

14. The method of claim 11 or 12, wherein a personalization application is encrypted with a secret symmetric key stored in a secured memory area of the device, a hash value of the personalization application is signed with a Secure Architecture Designer's private key, the encrypted personalization application and the signed hash value are loaded into the device, the personalization application is decrypted with the secret symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area.

15. The method of claim 11 or 12, wherein a personalization application and a hash value of the personalization application signed with a Secure Architecture Designer's private key are encrypted with a secret symmetric key stored in a secured memory area of the device, the encrypted personalization application and signed hash value are loaded into the device, the personalization application and signed hash value are decrypted with the secret symmetric key, the signature of the hash value is checked with the Secure Architecture Designer's public key stored in the read only memory of the device, and the personalization application is executed to write sensitive personalization data into the secure memory area.

16. A method according to any of the preceding claims, characterized in that the external memory includes a RAM and the chip has a bi-directional encryption/decryption hardware interface ensuring high performance and yet encrypted exchange of data between the chip and the RAM.

17. A device for executing applications that involve conditional access to at least one of valuable contents and services, including an integrated circuit that has a central processing unit, an internal memory and input/output connections for external memory incorporated on a single chip,

characterized in that the internal memory includes a secured memory area accessible to the central processing unit only and containing a secret encryption key used for encryption of sensitive data stored in the external memory.

18. The device according to claim 17, wherein said chip includes a random number generator.

19. The device of claim 18, wherein a hash value is obtained from a random number generated by the random number generator, the random number with its hash value are encrypted with said secret key, and the encrypted random number with its hash value are and stored in the external memory.

20. The device according to any of claims 17 to 19, wherein encryption is limited to sensitive application code and data.

21. The device according to any of claims 17 to 20, wherein said external memory is a flash memory.

22. The device according to any of claims 17 to 21, wherein a secret device key associated with each particular device is stored in said secured memory area, sensitive data are encrypted with said secret device key, the encrypted sensitive data are stored in the external memory and the encrypted sensitive data in the external memory are decrypted and verified at least at each reset of the device.

23. The device according to any of claims 17 to 22, wherein said secured memory area includes a signature verification public key used for verification of a signature attached to application code to be executed by the device.

24. The device according to any of claims 17 to 22, wherein application code to be executed by the device is stored in said external memory with an attached signature and with a signature verification key encrypted with a private key, a corresponding public key being stored in the read only memory of the device.

25. The device of claim 23 or claim 24, wherein an encrypted hash value of sensitive application code and data is added to application code stored in said external memory.

26. The device according to any of claims 17 to 25, wherein said secured memory area includes personalization data pertaining to an intended use, an intended customer and an intended configuration of the device.

27. The device according to claim 26, wherein said external memory includes an application code storage into which application code can be loaded subject to compliance with said personalization data.

28. The device according to any of claims 17 to 27, wherein said secured memory area is loaded with at least one secret key and a hash value of the content of the secured memory area prior to delivery of the chip to a customer.

29. The device according to any of claims 17 to 28, wherein the chip comprises intrusion detection means for, in response to a detected intrusion, erasing at least essential parts of said secured memory area.

30. The device according to any of claims 17 to 29, wherein the chip includes a watch-dog and the chip is reset or at least essential parts of said secured memory area are erased when no activity is detected by the watch-dog within a predetermined time.

31. The device according to any of claims 17 to 30, wherein the chip includes a clock monitor and any abnormal variation of the chip clock rate causes the chip to reset or at least essential parts of said secured memory area to be erased.

32. The device according to any of claims 17 to 31, wherein said chip has outer connection terminals that are variably assigned to internal connections, and a secret terminal assignment is used to supply secret keys and/or procedures to said memory.

33. The device of any of claims 17 to 32, comprising a read only memory area that contains mandatory authenticity verification code allowing an application to be executed by the device only after successful verification of authenticity, the secret memory area also containing authenticity verification data, and wherein said authenticity verification code is contained in a boot procedure.

34. The device of claim 33, wherein said internal memory includes a ROM and at least part of said authenticity verification data is obtained by applying a predetermined hash function to at least a predefined part of the ROM content.

35. The device of claim 34, wherein said authenticity verification code applies said predetermined hash function to said predefined part of the ROM content and compares the hash value with a corresponding part of the authenticity verification data.

36. The device according to any of claims 33 to 35, wherein said at least part of said authenticity verification data is obtained by applying a predetermined hash function to the content of the secured memory area.

37. The device of claim 36, wherein said authenticity verification code applies said predetermined hash function to the content of the secured memory area and compares the hash value with the corresponding part of the authenticity verification data.

5